Claim Rejections under 35 U.S.C. § 103

The Examiner rejected Claims 3-18 under 35 U.S.C. § 103 (a) as being unpatentable over Zimmerman et al., U.S. Patent No. 6,526,131 (hereinafter the "Zimmerman reference") in view of a printed publication entitled, "Introduction to SSL," (hereinafter the "SSL reference") allegedly published on October 9, 1998 and retrieved from the Internet on May 19, 2004 at: http://developer.netscape.com/docs/manuals/security/sslin/contents.htm.

The Applicants will address each independent claim separately as the Applicants believe that each independent claim is separately patentable over the prior art of record.

Independent Claim 3

It is respectfully submitted that the Zimmerman and SSL references and the Published '321 standard fail to describe, teach, or suggest the combination of (1) receiving a first message via HTTP from a client Internet telephony device that comprises (2) an automated request to obtain an identity of one of an Internet telephony clearinghouse and Internet telephony routing policy server, the request further comprising (3) an automated computer programming variable operation (4) that is set equal to alphanumeric text comprising 'getcacert' and that (5) initiates a search for a certificate authority certificate; (6) responding to the request by (7) transmitting a second message comprising the (8) certificate authority certificate of one of (9a) an Internet telephony clearinghouse and (9b) Internet telephony routing policy server (10) in a Base64 format and (11) encoded in ASCII with content type set to text/html; (12) receiving a third message comprising (13) a certificate request from the client Internet telephony device; (14) responding to the client Internet telephony device request (15) by signing the certificate; and (16) transmitting a fourth message comprising (17) the certificate signed by (18) a certificate authority of one of (19a) the Internet telephony clearinghouse and (19b) the Internet telephony routing policy server, as recited in amended independent Claim 3.

The Zimmerman Reference

The Zimmerman reference describes ways to avoid the need for dedicated PTSN phone lines. Dedicated PTSN phone lines can be phone lines used to keep two computer systems permanently connected for immediate communication between the two systems when required. A dedicated phone line is a simple, convenient and secure way to connect two systems.

Meanwhile, the Zimmerman reference describes a way to have the functional capabilities of a dedicated connection using a dial-up connection or another connection method that is used only when needed. The Zimmerman reference relates to remotely waking up customer premises equipment to cause the latter to initiate communication with a network-based service system.

The Zimmerman reference describes ways to use a wake-up call to a remote device to quickly establish a connection, rather than maintaining a dedicated phone line. The wakeup call is identified by means of a characteristic caller ID or distinctive ring, or, in the event the call is picked up, by rapid call termination, by an in-band signal, or by a predetermined period of silence. All these call characteristics permit the customer premises equipment to recognize wakeup calls on a line also receiving normal telephone calls.

The Examiner refers the Applicants to Column 8, lines 37-45 of the Zimmerman reference that generally describes the use of Secure Sockets Layers (SSLs) to establish secure communications. However, this section of the Zimmerman reference does not provide any further details about how SSL is used. In fact, the Examiner admits that the Zimmerman reference does not teach the specifics of the SSL protocol. See Office Action of August 20, 2004; page 2, paragraph number 4.

In light of this, it is apparent to one of ordinary skill in the art that the Zimmerman reference cannot anticipate nor render obvious a combination of elements noted above, especially (a) receiving a first message via HTTP from a client Internet telephony device that comprises (b) an automated request to obtain an identity of one of an Internet telephony clearinghouse and Internet telephony routing policy server, the request further comprising (c) an automated computer programming variable operation (d) that is set equal to alphanumeric text comprising 'getcacert' and that (e) initiates a search for a certificate authority certificate, as recited in amended independent Claim 3.

The SSL reference

The Examiner admits that the Zimmerman reference does not teach the specifics of the SSL protocol. To make up for this SSL deficiency, the Examiner relies on the SSL reference.

The SSL reference generally teaches the SSL protocol. The SSL provides a summary of steps that are taken during an SSL handshake to establish a secure communications channel. However, the SSL reference does not provide any teaching or description of the contents of

messages that are exchanged between a client device and a server. See the SSL reference on page 6, second full paragraph after the table which states the following:

> "The exact programmatic details of the messages exchanged during the SSL handshake are beyond the scope of this document. However, the steps involved can be summarized as follows (assuming the use of cipher suites listed in Cipher Suites with RSA key exchange):"

Therefore, it is apparent to one of ordinary skill in the art that the SSL reference, like the Zimmerman reference, also cannot anticipate nor render obvious a combination of elements noted above, especially (a) receiving a first message via HTTP from a client Internet telephony device that comprises (b) an automated request to obtain an identity of one of an Internet telephony clearinghouse and Internet telephony routing policy server, the request further comprising (c) an automated computer programming variable operation (d) that is set equal to alphanumeric text comprising 'getcacert' and that (e) initiates a search for a certificate authority certificate, as recited in amended independent Claim 3.

Published '321 Standard

As noted above by the Applicants, the Examiner did not use the Published '321 standard to reject any of the claims in the May 23, 2005 Office Action. However, the Examiner requested the Applicants during the telephonic interview of October 6, 2005 to explain how the Published '321 standard is different from the claimed technology. As a courtesy, the Applicants offer the following explanation in response to the Examiner's request.

The Published '321 standard has the following title: "Open Settlement Protocol (OSP) for Inter-Domain pricing, Authorization and Usage exchange." The Open Settlement Protocol (OSP) defines a standard set of messages that telephone carriers can use to authorize and account for inter-carrier telephone calls over IP networks. OSP messages are usually written in XML (eXtensible Markup Language) using text characters and English words and abbreviations.

Example OSP messages are AuthorizationRequest (a message which defines how to request the IP address corresponding to a telephone number) and UsageIndication (an accounting message which reports how call duration after the call is finished).

The OSP standard does not define any security or cryptographic techniques. However, the OSP standard does mention how OSP messages could be secured with existing cryptographic techniques in three places:

1) The OSP standard in section 5.1, page 13, defines that OSP messages written in XML may be conveyed using the Hyper Text Transport Protocol (HTTP) over an Internet Procotol (IP) network. The OSP standard also states that for secure communications, the OSP messages written in XML may also be transmitted using the Secure Sockets Layer (SSL) or Transport Layer Secure (TLS) protocol.

2) Annex B, page 46, of the OSP standard references cryptographic algorithms required by SSL/TLS and digitally signed messages and tokens.

3) Annex D, page 50, defines the format for OSP authorization tokens which may cryptographically encoded.

While these three security techniques rely on digital certificates, the OSP standard and the reference security technologies (SSL/TLS) do not teach how to exchange a digital certificate between and server and a client. As discussed with the Examiner during the telephonic interview of October 6, 2005, a certificate can be exchanged between a client and a server via any number of obvious mechanisms such as through U.S. Postal service (mail), E-mail, File Transport Protocol (ftp), and other like mechanisms. However, none of these mechanisms are practical for voice over Internet Protocol (VoIP). The inventive claims define an efficient operation which enable a VoIP client to automatically 'enroll' with a certificate authority. Enrollment usually includes obtaining a public key and signed certificate from a certificate authority.

In light of the differences between amended Claim 3, the SSL, Zimmerman references, and the Published '321 standard, one of ordinary skill in the art recognizes that the broadest, reasonable interpretation of these references cannot anticipate or render obvious the recitations as set forth in amended independent Claim 3. Accordingly, consideration and an indication that amended Claim 3 is allowable over the prior art are respectfully requested.

Independent Claim 7

It is respectfully submitted that the Zimmerman and SSL references and Published '321 standard fail to describe, teach, or suggest the combination of (1) receiving a first message from a (2) client Internet telephony device that comprises (3) an automated request to obtain an

identity of one of (4) an Internet telephony clearinghouse and (5) Internet telephony routing policy server; (6) responding to the automated request by (7) transmitting a second message comprising (8) a certificate authority certificate of one (9a) of an Internet telephony clearinghouse and (9b) Internet telephony routing policy server to the client Internet telephony device; (10) receiving a third message comprising (11) a certificate request from the client Internet telephony device, the certificate request comprising (12) a nonce value, (13) a user's name, (14) a user's password, (15) an Internet telephony device identifier, (16) a customer identifier, and a (17) certificate request to be signed; (18) responding to the client Internet telephony device request by (19) signing the certificate; and (20) transmitting a fourth message comprising (21) the certificate signed by the certificate authority of one of (22a) the Internet telephony clearinghouse and (22b) Internet telephony routing policy server., as recited in amended independent Claim 7.

As noted above in the discussion of independent Claim 3, the Zimmerman and SSL references and the do not address exact programmatic details of the messages exchanged during an SSL handshake. Therefore, it is apparent to one of ordinary skill in the art that the SSL reference and Zimmerman references cannot anticipate nor render obvious a combination of (a) receiving a third message comprising a certificate request from the client device, the certificate request comprising a (b) nonce value, a (c) user's name, a (d) user's password, a (e) device identifier, a (f) customer identifier, and a (g) certificate request to be signed; (h) responding to the client device request by signing the certificate; and (i) transmitting a fourth message comprising the certificate signed by the CA of the clearinghouse or routing policy server, as recited in amended independent Claim 7.

In light of the differences between amended Claim 7 and the SSL and Zimmerman references and the Published '321 standard, one of ordinary skill in the art recognizes that the broadest, reasonable interpretation of these references cannot anticipate or render obvious the recitations as set forth in amended independent Claim 7. Accordingly, consideration and an indication that Claim 7 is allowable over the prior art are respectfully requested.

Independent Claim 13

It is respectfully submitted that the Zimmerman and SSL and Published '321 standard references fail to describe, teach, or suggest the combination of (1) receiving a first message

from a client Internet telephony device that comprises (2) an automated request to obtain an identity of one of (3a) an Internet telephony clearinghouse and (3b) Internet telephony routing policy server; (4) responding to the request by (5) transmitting a second message comprising a certificate authority certificate of one of (6a) an Internet telephony clearinghouse and (6b) an Internet telephony routing policy server to the client Internet telephony device, wherein the second message comprises (7) a programming variable status that is set equal to alphanumeric text (8) comprising '0&certificate' that (9) indicates certificate authority information follows the alphanumeric text; (10) receiving a third message comprising a certificate request from the client Internet telephony device comprising a certificate request to be signed; (11) responding to the client Internet telephony device request by signing the certificate; and (12) transmitting a fourth message comprising (13) the certificate signed by the certificate authority of one of (14a) the Internet telephony clearinghouse and (14b) Internet telephony routing policy server, as recited in amended independent Claim 13.

As noted above in the discussion of independent Claim 3, the Zimmerman and SSL references and Published '321 standard do not address exact programmatic details of the messages exchanged during an SSL handshake. Therefore, it is apparent to one of ordinary skill in the art that the SSL reference, like the Zimmerman reference, also cannot anticipate nor render obvious a combination of (a) responding to the request by transmitting a second message comprising a certificate authority certificate of one of a clearinghouse and a routing policy server to the client device, wherein the second message comprises (b) a programming variable status that is set equal to (c) alphanumeric text comprising '0&certificate' that indicates certificate authority information follows the alphanumeric text; (d) receiving a third message comprising a certificate request from the client device comprising a certificate request to be signed; and (e) responding to the client device request by signing the certificate, as recited in new independent Claim 13.

In light of the differences between amended Claim 13 and the SSL and Zimmerman references, one of ordinary skill in the art recognizes that the broadest, reasonable interpretation of these references cannot anticipate or render obvious the recitations as set forth in amended independent Claim 13. Accordingly, consideration and an indication that Claim 13 is allowable over the prior art are respectfully requested.

New Dependent Claims 4-6, 8-12, and 14-18

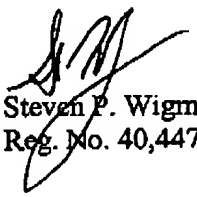
These dependent claims should be allowable because their corresponding independent claims should be allowable over the prior art of record. Consideration of these dependent claims and an early notice of allowance are courteously solicited from the Examiner.

CONCLUSION

The foregoing is submitted as a full and complete response to the Office Action mailed on May 23, 2005. The Applicants and the undersigned thank Examiner Jung for the consideration of these remarks. The Applicants have submitted remarks to traverse the pending rejections and to identify the differences between new Claims 3-18 and the prior art. The Applicants respectfully submit that the present application is in condition for allowance. Such Action is hereby courteously solicited.

If any issues remain that may be resolved by telephone, the Examiner is requested to call the undersigned at 404.572.2884.

Respectfully submitted,



Steven P. Wigmore
Reg. No. 40,447

King & Spalding LLP
45th Floor
191 Peachtree Street, N.E.
Atlanta, Georgia 30303
404.572.4600
K&S Docket: 06949.105013